NAVAL WAR COLLEGE
Newport, R.I.

The Double Edged Sword: Information Superiority or Information Vulnerability of Joint Vision 2010

by

Nancy L. Tanner
Commander, United States Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: Nancy L. Tanner

February 13, 1997

Roger W. Barnett
Professor Naval Warfare Studies

Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): The Double Edged Sword: Information Superiority or Information Vulnerability of Joint Vision 2010. (U)	
9. Personal Authors: CDR Nancy L. Tanner, USN	
10. Type of Report: FINAL	**11. Date of Report:** 13 February 1998
12. Page Count: 29	
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Information warfare, Operational Risk Assessment, information superiority, information infrastructure, Risk Assessment, information operation,	

15. Abstract: Joint Vision 2010 emphasizes the criticality of achieving Information Superiority in future military operations. With the global explosion of "Information Age" technology, the United States seeks a strategic and operational advantage through information while simultaneously denying an enemy any advantage. With no peer competitor to challenge the United States, adversarial nations may attempt to leverage the low cost, compared to high advantage, that information warfare has to offer. As the United States becomes increasingly reliant on the rapid flow of information, will the underlying infrastructure and deterrence effort provide sufficient security to ward off potentially devastating information warfare attacks?

Operational Risk Management (ORM) is a methodology to identify hazard severity and probability from which to draw reasonable measures to reduce risk. (ORM) techniques can be adopted to assess information warfare (defense) hazards and assist in developing controls to minimize risks. Recommendations highlight the importance of educating personnel in information warfare, incorporating information warfare (defense) in war games, studying information infrastructure issues and applying ORM principles to reduce vulnerabilities.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17. Abstract Security Classification: UNCLASSIFIED	
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT	
19. Telephone: 841-6461	**20. Office Symbol:** C

Security Classification of This Page Unclassified

ABSTRACT

Joint Vision 2010 emphasizes the criticality of achieving Information Superiority in future military operations. With the global explosion of "Information Age" technology, the United States military seeks to gain a strategic and operational advantage through information while simultaneously denying an enemy any advantage. With no peer competitor to challenge the United States, adversarial nations may attempt to leverage the low cost, compared to high advantage, that Information Warfare has to offer. As the United States military becomes increasingly reliant on the rapid and accurate flow of information, will the underlying infrastructure and deterrence effort provide sufficient security to ward off potentially devastating Information Warfare attacks?

Operational Risk Management (ORM) is a methodology to identify hazard severity and probability from which to draw reasonable measures to reduce risk. ORM techniques can be adopted to assess Information Warfare (defense) hazards and assist in developing controls to minimize risks. Recommendations highlight the importance of educating personnel in Information Warfare, incorporating Information Warfare (Defense) in war games, studying information infrastructure issues and applying ORM principles to reduce vulnerabilities.

TABLE OF CONTENTS

The Double Edged Sword: Information Superiority or Information Vulnerability of Joint Vision 2010

With Joint Vision 2010's emphasis on achieving Information Superiority, what Information Warfare threats may confront the operational commander and what measures can be implemented to reduce vulnerabilities?

INTRODUCTION

Information has been recognized as a crucial element in warfare for thousands of years. Sun Tzu recommended, "Know your enemy and know yourself; in a hundred battles you will never be in peril." [1] Even though the importance of information has been well known since ancient times, technological advances that have increased the speed and the ability to gather, manipulate, analyze, and disseminate information is a comparatively recent development. Is Information Warfare a bloodless method that satisfies the exhortation: "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."? [2] If Sun Tzu's wisdom is extrapolated to include advanced technology, will his concepts imply that the warrior who has information superiority will triumph over an adversary, or might information superiority also become a double edged sword -- proficient at inflicting devastating injury not only on the enemy but also on those who wield the sword?

BACKGROUND

Information Superiority

Joint Vision 2010 and Concept for Future Joint Operations Expanding Joint Vision 2010 were created to "... provide a conceptual framework for America's armed forces to think about the future." [3] One of the critical precepts of Joint Vision 2010 is the development of Information Superiority.

> We must have Information Superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information Superiority will require both offensive and defensive Information Warfare (IW). [4]

Joint Vision 2010 continues in its discussion of various methods of utilizing offensive Information Warfare against an adversary, and then cautions: "...our effort

to achieve and maintain Information Superiority will also invite resourceful enemy attacks on our information systems. Defensive Information Warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead." [5]

Information Warfare (IW)

With the incorporation of developments in technology, Information Warfare is a relatively new concept. As recently as 1994, that year's edition of the Department of Defense Dictionary of Military and Associated Terms had no definitions of information systems, Information Warfare, or Information Superiority. It does contain a definition of *information* but it is very rudimentary and relates more to intelligence, "...unprocessed data...used in the production of intelligence...." [6], than to the proliferation of automated systems that are in existence just three years later. Although the definition of Information Warfare is subject to change, it is broadly defined as:

> Actions taken to achieve Information Superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. [7]

Methods are being examined to utilize Information Warfare against an adversary, but those same concepts can be used offensively on the United States. The director of counter-information technology and programs of Martin Tactical Aircraft Systems, Robert McGuffee, summed up the danger of information weapons. "I typically look at an IW offensive technique...as having an operationally useful half-life of about two years. The first time I use it, it's going to take the enemy about two years to figure out what we did to him. I give an adversary two years to turn the

same weapon on us; therefore, four years from the time we use it, we'd better have a defense for all our own platforms." [8] Since Information Warfare can pose a threat, what are the foremost challenges confronting the operational commander in defensive Information Warfare, and how can those challenges be effectively mitigated?

CHALLENGES AND ISSUES IN INFORMATION WARFARE (DEFENSE)

> No nation is more vulnerable than the United States to electronic attacks, nor apparently, more reluctant to confront this potentially disabling weakness. Practices, procedures and technologies that materially would help defend against such attacks are known but largely ignored because of apathy, fear, ignorance and arrogance. None of this augurs well for a war fighting strategy that depends so absolutely on the integrity of information systems. [9]

Lack of a Peer Competitor

With the demise of the Cold War there is currently no peer competitor opposing the U.S. position of dominance as the premier military world power. Analysts generally project that a peer competitor will not emerge to challenge the United States military superiority until approximately the year 2012 or after. It is also assumed, by analysts, that the United States will be the only nation poised to exploit the full military technical spectrum, or Revolution in Military Affairs, that is anticipated over the next decade. [10] If these projections are valid, then why should operational commanders be concerned about possible attacks by adversarial information warriors? The timeless advice of Sun Tzu offers a warning: "It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible." [11]

Examples of information attack include: physical or electronic attacks on data, communication systems, hardware or software, cable connections, power grids, other information infrastructure, and deception to mask that any information was obtained, altered, or destroyed. Viruses could be surreptitiously entered into systems or critical data could be corrupted causing a network to fail at the most inopportune time. [12]

Asymmetrical Warfare

For the very reason that there are no peer competitors with an equivalent military force to match the United States, nations that seek to challenge the U.S. must leverage a low cost means of exploitation to gain a disproportionately sizable advantage. Information Warfare provides that capability. It is relatively inexpensive and does not require elaborate equipment to launch an attack, yet it offers the potential of high rates of return. Information Warfare is also very "stealthy"; it is difficult to ascertain from what nation(s) or group the attack emanated and therefore determine what nation(s) to deter from an attack or against which to initiate a counterattack. Defense officials acknowledge there are currently at least eight nations that present a substantial information threat to the United States. [13] There is also currently very little guidance in international law that specifically addresses Information Warfare. In seeking consensus on rules to govern various aspects of information, including Information Warfare, there is a large gap between the rapid growth of information infrastructure as compared to the slow enactment of law.

Law and Infrastructure

Criminal law, international law, and the law of armed conflict especially have not kept pace with the rapid escalation of innovation in the "Information Age". Can

attacks on information be considered warfare? Will Information Warfare satisfy international requirements of applying force only under just cause, with right intentions, directed by a legitimate authority, and meet the tests that the application of force is reasonably expected to produce success, for the purpose of good, be taken only as a last resort, and taken with the expectation that peace will be the outcome? Additionally the United Nations Charter requires that the use of force should only be invoked in self-defense. [14] Will a terrorist group or potential enemy pause to contemplate these tests before launching an information assault designed to disrupt the national security of the United States?

Along with these issues is the fact that much of the military's information needs and communication requirements are leased or purchased from civilian commercial entities. More than 90 percent of communications used by the Department of Defense are operated by civilian systems. [15] If one were to use cost estimates to provide a relative comparison in size between information infrastructures, one would find that the Defense Information Infrastructure (DII) at $23 Billion (B) is a little more than half the size of the Government Services Information Infrastructure (GSII) at $40 B, significantly less than the National Information Infrastructure (NII) at $500 B, and dwarfed by the Global Information Infrastructure (GII) at $1000 B. These infrastructures are not mutually exclusive; there is a considerable amount of overlapping and interdependencies. [16]

The backbone of military communication and information infrastructure is inextricably intertwined with the civilian infrastructure. The military has no control of the integrity or security of this underling infrastructure. There is a recognition, at upper levels of the government, that the "Information Super Highway" is crucial to the nation, but due to privacy concerns and the desire for government deregulation, oversight and control lies in the civilian sector. Managed piecemeal by an

aggregate of diverse civilian corporations and operated by the dictums of disparate commercial enterprises, the nation's information infrastructure is an organic entity with no centralized leadership. Even though the Internet originated as the ARPANET in 1969 as a military network of 4 computers, it has rapidly expanded to over 58 million users and is expected to increase by 183 percent each year. Spanning 135 countries and over 9.5 million computers the DoD is now just one of many customers on the Internet, and definitely not in control. [17]

Because of the ambiguity of laws and the diffusion of responsibility for managing the nation's information infrastructure, it is difficult to develop defense/deterrence strategies and response options to protect critical information infrastructures. [18] The Defense Science Board highlighted the problems of the nation's infrastructure in its 1996 report:

> Information infrastructures are vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope and potential of the Information Warfare threat. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict. [19]

Paradigm Paralysis

Additionally, Information Warfare is so new and unexplored it does not fit general paradigms of warfare, and therefore people tend to be reluctant to view Information Warfare as a threat or comprehend the disruption of which it is capable. Information Warfare does not shoot and kill people outright, but it has the potential to disrupt information and communication systems that are critical to military operations. This reluctance alone is a problem because in general, people do not sufficiently prepare for a threat that is considered unlikely -- especially under time or resource constraints. An everyday example involves the use of seat belts based

on perceived risks. Some people who religiously buckle their seat belts for long highway trips fail to do so on short hurried trips to the neighborhood store. The rationale is that the risk is not high for a short, low speed trip. In reality, accidents can occur on the shorter trip and could be just as deadly without the seat belt.

After the end of the Cold War, military forces and budgets were downsized, which forced reassessments of how to safeguard national interests and simultaneously develop methods to drive down costs in order to "cash in" on the "peace dividend".

Cost Savings Versus Security

One of the methods to drive down costs was to take advantage of Commercial Off-The-Shelf (COTS) hardware and software. With rapid advances in the information age, software and hardware products became readily available commercially. Acquisition costs of information technology could be lowered if software and hardware could be procured through commercial vendors as opposed to programming or building "from scratch" to meet Military Specifications (MILSPECS). Standardization was a benefit to this methodology as well as cost savings; but on the down side, security of information may suffer. A larger proportion of hardware and software used by the military today is available on the open market, which invites exploitation by those who would attempt to infiltrate a system or network. The tradeoff becomes a question of cost savings or security. Once again, if the perception is that the risk is low, then precautions may not be implemented.

Chance and Risk

> War is the realm of chance.... Chance makes everything more uncertain and interferes with the whole course of events. Since all information and

assumptions are open to doubt, and with chance at work everywhere, the commander continually finds that things are not as he expected. [20]

As Clauswitz remarked, the uncertainty of events, or chance, is an element operational commanders must deal with on a routine basis. Whether in peace, war, Military Operations Other Than War (MOOTW), or even in simple daily activities, chance plays a role. If things are left to chance and measures are not taken to lessen risks, luck may reign. The United States cannot afford to leave national defense or critical information infrastructure to the whim of luck.

In a Congressional Committee meeting in June 1991, Winn Schwartau told the members: "Government and commercial computer systems are so poorly protected today that they can essentially be considered defenseless -- an electronic Pearl Harbor waiting to happen." [21]

Information Infrastructure and Titanic Compared

Another analogy could be made comparing the information infrastructure to the *Titanic*. People erroneously thought that technology was so advanced that the ship was unsinkable. (Information Superiority is sometimes thought to mean infallibility. Even though risks might not have a high probability of occurrence there is still no method to totally remove risk from an operation.) In theory the watertight doors in the *Titanic's* bulkheads would limit the risk of flooding to just a few compartments and the ship would not founder. In reality the watertight doors were just oriented in a vertical position and did not seal horizontally between decks . Water was able to overflow the top of the doors and cascade into the next compartment. (Security measures and firewalls are thought to be in place on computer networks but the "back doors" that allow entry to authorized programmers to troubleshoot the system also allow entry by those who seek to disrupt the

system.)

Beyond the watertight doors, "backup" systems were not considered essential on the *Titanic*. There were lifeboats for only approximately half the people on board the ship. The number of lifeboats complied with the laws of the time, based on the gross tonnage of the ship -- not as one would think, on the number of seats required. This was also an economic consideration and perhaps a statement to assuage anyone's doubts of the ship's unsinkable image. (Are information systems, that operational commanders rely upon, sufficiently redundant based on risk assessment? Are there contingency plans to safeguard critical hardware and backup / recover information?)

In 1907, *Titanic's* Captain, Edward J. Smith, was quoted as saying, "When anyone asks me how I can best describe my experiences of nearly forty years at sea, I merely say, 'Uneventful.'" [22] Ice warnings were received by the *Titanic*, but since Captain Smith had not previously had a "close call" with an iceberg perhaps the warnings were not taken as seriously since they had not posed a threat in his 40 years of service. An extra lookout was posted, but neither man was issued binoculars, and the speed of the ship was not reduced. (Information Warfare is relatively new, high ranking military officers with many years of experience may not have witnessed Information Warfare used against U.S. forces and therefore perhaps do not respect its potential for disruption. Are we halfheartedly looking for Information Warfare threats on the horizon? Have we given observers the tools to identify intrusions, or are we just in a hurry to get where we are going, no matter what the risk?)

In the era of the *Titanic*, communication units on ships were not manned 24 hours. A potential rescue ship, the Californian, in close proximity to the *Titanic*, never heard the distress call because the one wireless operator on board had

gone to sleep. (Reports of intrusion into information systems are often not detected because people are not monitoring systems to detect unauthorized access, perhaps potential intrusions are not considered to be possible or not thought to be a threat.) The *Titanic* was the first to use the new distress signal SOS, it also used the more recognized signal CQD. They wanted to be heard. (In contrast, information attackers will rely on stealth, and try to escape disclosure, this is often aided by the fact that when intrusions are detected they are not reported to authorities. Is this because those who detect the intrusion have difficulty interpreting the discovery or do not want to explain how someone could infiltrate the supposedly inaccessible system? "Department of Defense computers were attacked an estimated 250,000 times in a single year, with most of the attacks going undetected." [23] A staggering result of a Defense Information Systems Agency (DISA) vulnerability assessment, was that of 38,000 mock attacks on DoD computers, entry was gained 65 percent of the time. Of those attacks that succeeded, only 988 (about four percent) were detected. Of the attacks that were detected, just 267 (about 27 percent) were reported to officials. [24])

The lifeboat davits on the *Titanic* were new and since the crew was unfamiliar with the new davits they lost precious time in launching the boats. (If not properly trained in identifying and reporting an intrusion, valuable time will be lost in dealing with intrusions or an outright information attack.)

When it was realized that the ship would sink within one to two hours, there was no established plan to evacuate the ship and prioritize the limited number of lifeboat seats. About 495 seats were left vacant and only 705 people were saved . (With the rapid proliferation of newly developed information systems, do these systems have realistic contingency plans and priorities *when* the systems fail, or suffer an attack, especially if the system has extensive interdependencies on other

government or private industry systems? For operational commanders, a plan may not exist to prioritize which functions are critical to military operations once dependent information systems or infrastructure fails. "During crises, the demand for information will increase; the infrastructure capacity will decrease. There is no mechanism in place to determine the priority of information requirements and allocate diminishing infrastructure capacity during such a crisis." [25])

Another problem that arose was the mind set that since the *Titanic* was a large new ship and touted as being unsinkable, why should anyone entrust his or her life to a small boat being lowered to the ocean, about half-way across the Atlantic, after midnight? Some stayed with the *Titanic* because it gave the illusion of being "safer". (Will operational commanders, subordinate commanders or staff personnel make a similar mistake in judgment? "The information we received must be true, that system has always been a reliable source and it is such a large, complex, and secure network why should we question the veracity of that information?" Could the information be disinformation inserted by a clever infiltration designed to deceive the operational commander's decisions on where to deploy forces?)

The analogy of the *Titanic* compared to the information infrastructure and the military's dependency on that infrastructure was used to illustrate that even though an event is unlikely, it could have profound repercussions *if* it does occur. Unfortunately in the case of the *Titanic*, it did occur with a devastating loss of life. The name *Titanic* became synonymous with tragedy and the arrogance that technology will overcome all obstacles. After the *Titanic*, laws were enacted to lessen maritime risks. The lesson of placing too much trust in technology is evident, but will we heed the "ice warnings" or do we need to experience the collision before we have the opportunity to make a course correction?

Risk Assessment

According to insurance assessments, the risk for total loss of a ship due to collision with an iceberg is a one-in-a-million, ***probability***. [26] The fact that the probability was low lulled decision makers into seeing no value in expending money on additional lifeboats. But not fully considered was an assessment of the level of ***severity*** if the event *did* occur. Given that the probability was low, the conclusion was reached that extra lifeboats were not a cost effective item. If the logic were applied that even though the probability was low (that the ship would sink) but if the event *did* occur the severity would be high (loss of thousands of lives), it would then be reasonable to expend at least some money for extra lifeboats. Risk can be better managed when both the ***mishap probability*** and ***hazard severity*** are taken into consideration. In this case the balance between cost and benefit would point to the fact that at a small cost of a few more lifeboats more people *could* be saved *if* the event occurred.

OPERATIONAL RISK MANAGEMENT (ORM)

The *Titanic* example highlights two of the elements of Operational Risk Management: mishap probability and hazard severity. Operational Risk Management is a methodology to manage risk by identifying hazards and providing reasonable measures to reduce risk. Risk management "...is usually highly reactive. We tend to identify only those hazards which have caused problems in the past." [27] (As was the case with Captain Smith of the *Titanic*, a one-in-a-million event that has not been personally experienced may not appear obvious.) ORM is a proactive process in that it identifies past hazards and offers a way to visualize and control threats that may not have been considered. The five steps of ORM are:

(1) Identify Hazards: Visualize events and identify problems.

(2) Assess Hazards: Identify which hazards present the greatest risks. Determine the probability the hazard will occur.

(3) Make Risk Decisions: Decide what controls can be used to counter the highest risk. Determine if the potential gain is worth the risk.

(4) Implement Controls: implement controls and any courses of action from step 3.

(5) Supervise: Monitor for effectiveness and correct ineffective controls. [28]

The ORM process can be conducted in several formats from the time critical 'mental walk though' of the five steps to an in-depth flowchart method. Various tools can be used to assist in the ORM process such as: Flow charting, Brainstorming, Simultaneously Timed Events Plotting (STEP), Affinity Diagram, Failure Mode and Effect Analysis, "What-if" Analysis, and Risk Assessment Matrix, to name just a few. [29]

Using a "What -if" scenario and a Risk Assessment Matrix to demonstrate the ORM process, similar techniques can be used to assess various risks of an Information Warfare threat to an operation.

Information Warfare Scenario

A nation hostile to the U.S. contracts a group of computer specialists from another country to design a program to disable and disrupt personal computers in the U.S. military. The ploy is to offer a game that features a war between the originating country and the United States. The game is placed on the Internet as freeware with options to play against others or against the computer . Because the game offers realistic scenarios against a real foe, the game takes on an unprecedented popularity with military personnel. People are competing to see

who can defeat the enemy, win the most points in the game, and have their name "immortalized" on the Internet scoreboard (if only for a few days). Even though rules prohibit games on military computers, the game is played on military computers. The game is thought to be harmless (no viruses are associated with it, so far) and the game is unofficially encouraged because it develops a keen sense of competition, boosts morale, and sharpens the troop's skills while they are preparing for the real confrontation with the adversary.

In reality though the "game" is a vehicle to "addict" as many personnel as possible into playing the game on military computers with the aim to eventually load a time bomb virus to "explode" on a specified day. As an extra benefit to the adversary nation, whenever an individual plays the game, logs on to retrieve a new version of the game, or logs on to brag about obtaining a high score; the adversary learns a little bit more about the way the United States might operate in a real confrontation. The enemy is using the game as a "war game simulation" to collect data on the courses of action the United States most likely will take. In some cases personnel opt to play the adversary and provide valuable insight on how to defeat the United States. Based on a survey that individuals must answer prior to playing the game, the adversary estimates, that 85 percent of military personnel in theater, or expected to be involved in the operation, have loaded the "game" on a desk top military computer.

When it becomes clear that an actual skirmish is imminent , a time bomb virus is placed in the next version on the Internet where it is unwittingly downloaded by those eager to try the newest version. The time bomb is set to detonate a day before the adversary will launch a massive conventional assault against U.S. forces. The time bomb virus will render computers it infects useless until an uninfected operating system and applications are loaded.

Given the scenario is an example of an event that could occur in the future, how might it be assessed for potential risks and what controls can be implemented to better manage those risks?

Scenario Risk Assessment

In using scenarios, it is helpful to look at the worst case possibilities. There are two potential hazards in the example:

(1) Computer disruption. Widespread desk top computer disruption will occur at a critical time.

(2) Data/Intelligence disclosed. Data is provided (unwittingly) to the enemy that can be synthesized into intelligence of U.S. strengths, weaknesses, and possible courses of actions.

In assessing the two problems the following questions need to be considered:

1. PROBABILITY: How likely is this hazard?
2. SEVERITY: What would be the severity of this hazard if it did transpire? (What is the worst thing that could happen?)
3. CONTROLS: What controls can be instituted to lessen the risk?

Without statistical data, some of the answers are subjective. The key is to not stop the process at the first question of probability because the hazard is thought to be "impossible". A Risk Assessment Matrix can aid in assessing the potential risks. A numerical Risk Assessment Code (RAC) from one to seven is defined by the two elements of Hazard Severity (vertical axis) and the Mishap Probability (horizontal axis). Risk control priorities are then derived from the Risk Assessment Code (RAC) in the matrix. Through discussions with staff personnel, including computer and intelligence specialists, it is assessed that for the computer disruption issue, the Mishap Probability is "High" and the Hazard Severity is" Medium" which would give an (RAC) of 3 , a Moderate Risk, according to the RAC legend in Figure 1.

Figure 1
Risk Assessment Matrix

	Mishap Probability				
Hazard Severity	Very High	High	Medium	Low	Very Low
Catastrophic	1	1	2	3	4
Critical	1	2	3	4	5
Medium	2	3	4	5	5
Marginal	3	4	5	5	6
Negligible	4	5	5	6	7

Risk Assessment Code (RAC) Legend:

1. Critical
2. Serious
3. Moderate
4. Low Risk
5. Minor Risk
6. Extremely Low risk
7. Negligible Risk

With a Risk Assessment Code of 3 or a "Moderate" hazard, controls to reduce the risk can be implemented and supervised to determine adequacy. In this case, automating virus checking routines and installation of updates to virus checking software along with emphasized training on virus threats, and random monitoring of computers for game software is conducted to lessen the threat. Another measure instituted is to isolate key computers from the Internet and casual "disk swapping" activities that may introduce a virus. Backup routines are monitored for compliance and original system software and application software and manuals are checked to ensure multiple copies are available if a degradation occurs.

Data/Intelligence disclosed: The unwitting disclosure of data has occurred in the past and has a potential to occur in the future thanks to the popularity, speed, and global nature of the Internet. A pilot that assisted in the rescue of downed pilot Captain Scott O'Grady in Bosnia wrote an e-mail to military friends describing the mission. "Within hours, sensitive (but not secret) details - including pilot code names, radio frequencies and weapons information - were available worldwide to 3 million America Online subscribers." [30] In this case the Mishap Probability is rated High and the Hazard Severity as Critical which would rank as a 2 or "Serious" risk and then appropriate controls can be derived and implemented.

While the activities discussed in the scenario might occur and cause potential disruptions at the operational level, there may also be disruptions that can occur at a strategic level.

An Additional Dilemma

To add to the complexity of the scenario, "what if" it is December 1999 and the 'year 2000 issue' which is predicted to pose problems on mainframe based government and civilian systems, actually does cause some instability. (The premise is that legacy mainframe based systems that use two digit dates i.e., "97" and require a conditional logic statement such as : 'if year XX , is greater than year YY, then do a certain routine'. The problem is the year 2000 will be represented as "00" and will be less than, rather than greater than "98".) Many of these old systems were programmed in COBOL, or other languages which programmers are no longer proficient in, thus presenting a challenge to make "software patches" with unknown results. Will this situation cause problems in the civilian, government, and military infrastructure? Might disruption occur in key transportation, communications, and logistics systems that are critical to military

operations? Might an adversary further exacerbate this weakness or use it to advantage?

Summary of Scenario Risk Assessment

As can be gathered from the scenario and assessment , Information Warfare, especially in the area of defense, requires further study. The United States may currently have the advantage in Information Warfare, but can it sustain the advantage past the year 2010, against persistent adversaries? One of the key elements in answering this question is based on another question: Is the United States fully aware of the situation? There are complex interdependencies that exist between information infrastructures and military operations. If operational commanders, or their subordinates, are not fully aware of potential vulnerabilities, the commander may discount the danger, thus resulting in a possible calamity that could have been avoided. Operational Risk Management offers a way to approach and resolve some of the Information Warfare issues confronting operational commanders.

One of the dictums of preparing for military operations is 'to train as you will fight'. If this is the case, then it is imperative to take Information Warfare, both Offensive and Defensive, into consideration when training and educating future warriors. The fact that "[T]he Naval War College has integrated Information Warfare play into its Global Games." [31] is a positive measure to ensure Information Warfare is seen as a viable instrument that can serve either side of the conflict.

CONCLUSION and RECOMMENDATIONS

Joint Vision 2010 provides the focus of Information Superiority as a desirable goal but much effort is required to ensure security of information systems

and infrastructure before superiority can be achieved . Obviously, with such complex interdependencies between the various information infrastructures, there are no "silver bullets" to ensure integrity. Broad actions that can assist the U.S. military in its quest for Information Superiority include efforts to:

1. Promote awareness of the complexities and potential vulnerabilities of the information infrastructure for better comprehension of the challenges.
2. Educate mid to upper level military personnel in Information Warfare and Operational Risk Management.
3. Instill Information Warfare (Defense) assaults in war games to exercise thought processes to deal with realistic challenges.
4. In concert with other civilian and government agencies, continue the process of studying critical information infrastructure issues and utilize Operational Risk Management methodology to identify risks and apply sufficient controls.

Even though risk cannot be totally eliminated, Operational Risk Management offers a methodology to visualize potential hazards and apply controls to reduce risks to an acceptable level. Whether the controls act to deter aggressors from using Information Warfare against the United States, assist in fortifying information infrastructures, or provide ideas to operational commanders to "outmaneuver" an imminent information attack, controls developed through Operational Risk Management can become effective mileposts on the journey toward the destination of Information Superiority.

Notes

[1]Sun Tzu, The Art of War, Samuel B. Griffith, trans. (Oxford: Oxford University Press, 1980) 84.

[2] ibid, 77.

[3] Concept for Future Joint Operations, Expanding Joint Vision 2010 (Washington, DC, 1997) i.

[4] Joint Vision 2010 (Washington, DC , 1996) 16.

[5] ibid.

[6] Joint Pub 1-02, DoD Dictionary of Military and Associated Terms (Wash. D.C. , 1994) 184.

[7] Joint Pub 3-13.1 (1996) GL8-9.

[8] David A. Fulghum, "Computer Warfare Offense Takes Wing," Aviation Week and Space Technology January 19,1998: 58.

[9] Col Alan D. Campen, USAF (Ret), "Rush to Information-Based Warfare Gambles with National Security," Signal July 1995: 68.

[10] Mary C. Fitzgerald, "The Russian Image of Future War," Comparative Strategy, Vol.13, No. 2, APR/JUN 94 issue ed.: 167.

[11] Sun Tzu, 114.

[12] Information Warfare; Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, 1996 ed.: (page 2-18).

[13] David A. Fulghum, "New Weapons Slowed By Secrecy Clampdown," Aviation Week and Space Technology January 19,1998: 54.

[14] Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force," Naval War College Review , (Spring98): 15.

[15] Kenneth A. Miniham, "Intelligence and Information Systems Security: Partners in Defensive Information Warfare," Defense Intelligence Journal, 5, no. 1 Spring 1996: 20.

[16] Information Warfare; Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, 1996 ed.: (page 2-15).

[17] Congress, Senate, Committee of Government Affairs, Permanent Subcommittee on Investigations, Hearings on Security in Cyberspace, (Minority Staff Statement), 104th Congress, 2nd session, 5 June 1996, 1-7.

[18] Information Warfare; Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, 1996 ed.: (page 1-5).

[19] Report of the Defense Science Board Task Force on Information Warfare Defense (Washington, D.C. , 1996) ES-2.

[20] Carl Von Clausewitz, On War, Michael Howard and Peter Paret eds. and trans. (Princeton: Princeton University Press, 1984) 101-102.

[21] Winn Schwartau, Information Warfare, Chaos on the Electronic Superhighway (New York: Thunder's Mouth Press, 1994) 13.

[22] Charles Hirshberg, "The Tragedy of the Titanic," Life June 1997: 66.

[23] Gary H. Anthes, "U.S. easy target for cyberattacks," Computerworld 30, no. 22 ,1996: 7 .

[24] Clarence A. Robinson Jr., "Western Infrastructures Face Rogue Data Stream Onslaught," Signal January 1997: 35.

[25] Information Warfare; Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, 1996 ed.: page 2-26.

[26] Lawrence Beesley, "The Loss of the S.S. Titanic, Its Story and Its Lessons," The Story of the Titanic as Told by its Survivors, Jack Winocour Ed. (New York: Dover Publications, Inc., 1960) 86.

[27] Reference Guide for Operational Risk Management, (Draft ed.) (: Naval Safety Center, 1997) 3.

[28] ibid, 3-5.

[29] ibid,1-5.

[30] Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," Washington Post July 16, 1995, : C-5.

[31] Information Warfare; Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, 1996 ed.: page 3-8.

BIBLIOGRAPHY

Books

Ballard , Robert D. The Discovery of the *Titanic.* Ontario, Canada: Madison Press Books, 1987.

Beesley, Lawrence. "The Loss of the S.S. Titanic, Its Story and Its Lessons," The Story of the Titanic as Told by its Survivors, Jack Winocour Ed. New York: Dover Publications, Inc., 1960.

Clausewitz, Carl Von. On War, Michael Howard and Peter Paret eds. and trans. Princeton: Princeton University Press, 1984.

Hruska, Jan. Computer Viruses and Anti-virus Warfare. London: Ellis Horwood Limited,1992.

Johnson, Stuart E. and Libicki, Martin. ed. Dominant Battlespace Knowledge. National Defense University, 1996.

Schwartau, Winn. Information Warfare, Chaos on the Electronic Superhighway New York: Thunder's Mouth Press, 1994.

Smith, Martin. Commonsense Computer Security, Your practical guide to information protection. New York: McGraw-Hill Book Co., 1993.

Sun Tzu. The Art of War, Samuel B. Griffith, trans. Oxford: Oxford University Press, 1980.

Periodicals and Articles

Anthes, Gary H. "U.S. easy target for cyberattacks." Computerworld 30, no. 22 ,1996: 7.

Barnett, Roger W. "Grasping 2010 with Naval Forces." Strategic Research Department, Research Report 2-97, U.S. Naval War College.

Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force," Naval War College Review , (Spring 98).

Campen, Alan D. Col USAF (RET), "Rush to Information-Based Warfare Gambles with National Security." Signal July 1995, 67-69.

Campen, Alan D. Col USAF (RET), "Information Warfare is Rife with Promise,Peril." Signal, November 1993, 19-20.

Dunlap, Charles J. Jr. "How We Lost the High Tech War of 2007." The Weekly Standard, January 29, 1996. Vol. 1, No.19; p 22.

Fitzgerald, Mary C. "The Russian Image of Future War," Comparative Strategy, Vol.13, No. 2, APR/JUN 94 issue ed., 167.

Fulghum, David A. "New Weapons Slowed By Secrecy Clampdown," Aviation Week and Space Technology January 19,1998: 54.

Hirshberg, Charles. "The Tragedy of the Titanic," Life June 1997: 66.

Miniham, Kenneth A. "Intelligence and Information Systems Security: Partners in Defensive Information Warfare," Defense Intelligence Journal, 5, no. 1 Spring 1996.

Munro, Neil "The Pentagon's New Nightmare: An Electronic Pearl Harbor," Washington Post July 16, 1995, : C-5.

Robinson, Clarence A. Jr., "Western Infrastructures Face Rogue Data Stream Onslaught," Signal January 1997: 35.

Robinson, Clarence A. Jr., "Information Warfare Demands Battlespace Visualization Grasp," Signal February 1997: 17-23.

Robinson, Clarence A. Jr., "Information Dominance Edges Toward New Conflict Frontier," Signal August 1994: 37-40.

Walsh, Edward J. "Technology Initiative Promises Improved Fleet Performance," Signal December 1997.

Government Documents

Charter of the United Nations, AFP 110-20, 27 July 1981. pp. 5-2 to 5-15.

Computers at Risk, Safe Computing in the Information Age. National Academy Press, 1991.

Concept for Future Joint Operations, Expanding Joint Vision 2010 Washington, DC, 1997.

Congress, Senate, Committee of Government Affairs, Permanent Subcommittee on Investigations, Hearings on Security in Cyberspace, (Minority Staff Statement), 104th Congress, 2nd session, 5 June 1996.

Cornerstones of Information Warfare. U.S. Air Force, 1995.

DoD Directive Number S-3600.1, Information Operations (IO), December 1996.

Joint Pub 1-02, DoD Dictionary of Military and Associated Terms ,Wash. D.C. , 1994.

Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W) Wash. D.C. ,1996.

Joint Vision 2010 ,Washington, DC , 1996.

Information Warfare; Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition, 1996 ed.

New World Vistas, Air and Space Power for the 21st Century, Information Application Volume. U.S. Air Force, 1996.

Planning Considerations for Defensive Information Warfare, Information Assurance. Prepared for Defense Information Systems Agency (DISA), 1993.

A Primer on Legal Issues in Information Warfare U.S. Air Force, 1995.

Reference Guide for Operational Risk Management, (Draft) Naval Safety Center, 1997.

Report of the Defense Science Board Task Force on Information Warfare Defense ,Washington, D.C. , 1996.

Unpublished Papers

Bishop, Roy V., Lieutenant Colonel USA. Information Operations: A Layman's Perspective. Unpublished research paper, Army War College, Carlisle Barracks, PA, 1997.

Hamby, Janice M. Commander USN. Operational Protection of Information Technology Assets, a Commander's Guide to Risk Reduction. Unpublished research paper, Naval War College, Newport RI, 1997.

Harley, Jefferey A. Lieutenant Commander USN. Information, Technology, and the Center of Gravity. Unpublished research paper, Naval War College, Newport RI, 1996.

Kirsch, Robert A. II, Lieutenant Colonel USA. Viruses and other Computer Pathogens: Should DoD Care? Unpublished research paper, Army War College, Carlisle Barracks, PA, 1997.

Leugers, Jerry W. , Commander USN. Information as an Operational Factor. Unpublished research paper, Naval War College, Newport RI, 1997.

Orr, Joseph E., Lieutenant Colonel USA. Information dominance: A Policy of Selective Engagement. Unpublished research paper, Army War College, Carlisle Barracks, PA, 1997.

Pears, Andrew H. Captain USAF. Planning for the Information Campaign. Unpublished research paper, Air University, Air force Institute of Technology, Wright-Patterson Air force Base, Ohio, 1996.

Ross, Mitchell, Lieutenant Colonel USA. National Information Systems: The Achilles Heel of National Security. Unpublished research paper, Army War College, Carlisle Barracks, PA, 1997.

Rowe, Wayne J. Information Warfare: A Primer for Navy Personnel. Research Report 6-95, Center for Naval Warfare Studies, U.S. Naval War College, Newport RI, 1995.

Stewart, Michael J., Lieutenant Colonel USA. Information Operations, Information Warfare: Policy Perspectives and Implications for the Force. Army War College, Carlisle Barracks, PA, 1997.

Straughan, Matt Commander USN. Information Operations and Unity of Effort, the case for a Joint Interagency Information Operations Task Force. Unpublished research paper, Naval War College, Newport RI, 1997.

Sweitzer, Wayne F. Commander USN. Battlespace Information, Command and Control (C2), Operational Intelligence, and Systems Integration. Unpublished research paper, Naval War College, Newport RI, 1997.

Vego, M. N. Operational Functions. Unpublished research paper, Naval War College, Newport RI, 1996.